Electronic Version

Stylesheet Version v1.1.1

Description

Method and apparatus for geometric key establishment protocols based on topological groups

Cross Reference to Related Applications

[0001] U.S. Pat. No 5,696,826,12/1997, by Gao; U.S. Pat. No 6,493,449,12/2002, Anshel et al; U.S. Pat. Application No 10/605,935, 11/2003, Berenstein and Chernyak.

Background of Invention

[0002] Description of the Prior Art: Key Establishment Protocols

[0003] The concepts, terminology and framework for understanding cryptographic key establishment protocols is given in Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone, "Handbook of Applied Cryptography," CRC Press (1997), pages 490-491.

[0004] A `protocol` is a multi-party algorithm, defined by a sequence of steps specifying the actions required of two or more parties in order to achieve a specified objective.

[0005] A `key establishment` protocol is a protocol whereby a shared secret becomes available to two or more parties, for subsequent cryptographic applications.

[0006] A `key transport` protocol is a key establishment protocol where one party creates or obtains a secret value, and securely transfers it to the other participating parties.

[0007] A `key agreement` protocol is a key establishment protocol in which a shared secret is derived by two (or more) parties as a function of information contributed by, or associated with, each of the participating parties such that no party can predetermine the resulting value.

[0008] A `key distribution` protocol is a key establishment protocol whereby the established keys are completely determined a priori by initial keying material.

[0009] The Diffie-Hellman key establishment protocol (also called `exponential key exchange`) is a fundamental algebraic protocol. It is presented in W. Diffie and M. E. Hellman, "New Directions in Cryptography," IEEE Transaction on Information Theory vol. IT 22 (November 1976), pp. 644-654. The Diffie-Hellman protocol provided the first practical solution to the key distribution problem, allowing two parties, never having met in advance or sharing keying material, to establish a shared secret by exchang-

ing messages over an open channel.

[0010] The security of this protocol rests on the intractability of the Diffie-Hellman problem and the related problem of computing discrete logarithms in the multiplicative group of the finite field GF(p) where p is a large prime, cf. Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone, "Handbook of Applied Cryptography," CRC Press (1997), page 113.

[0011] Most of known applications of Diffie-Hellman protocol deal with finite groups. Recently there emerged versions of Diffie-Hellman protocol for infinite, but yet discrete groups (see for example, US Patent N*6,493,449* by Anshel et al).

[0012] Unlike approaches existing in the prior art, the present invention is based not on finite or discrete groups, but rather on the connected compact topological groups.

[0013] Brief overview of connected compact topological groups

[0014] The basic reference for concepts, terminology and historical framework in topological group are given in the monograph by Philip J Higgins, *Introduction to topological groups*, Cambridge : University Press, 1974, and in the monograph by John F. Price, *Lie groups and compact groups* , Cambridge [Eng]; New York : Cambridge University Press,

1977.

[0015] A *group* (G,*) is defined as a set G together with a binary operation *: G ×G → G satisfying the following axioms:

[0016] *Associativity*: For all a, b and c in G, $(a * b) * c = a * (b * c)$.

[0017] *Identity element*: There is an element e in G such that for all a in G, $e * a = a = a * e$.

[0018] *Inverse element*: For all a in G, there is an element b in G such that $a * b = e = b * a$, where e is the identity element from the previous axiom.

[0019] A *topological group* G is a group which is also a topological space such that the group multiplication G ×G → G and the operation of taking inverses G → G are continuous maps. (Here, G ×G is viewed as a topological space by using the product topology).

[0020] A topological group G is called *compact* if the underlying topological space is compact, i.e., if any open cover of the space G has a finite sub-cover.

[0021] A first example of compact topological groups is any finite group (equipped with the discrete topology). Such groups provide examples of compact disconnected topological groups.

[0022] Another class of compact topological groups is *connected* compact topological groups. A topological group is *con-*

nected if the underlying topological space is connected. This class contains such groups as SO(V), where SO(V) is the group of all special orthogonal transformations of a Euclidean vector space V (therefore, there are at least as many compact connected topological groups as there are Euclidean vector spaces).

[0023] The present invention implements the ideas and algorithms of Diffie-Hellman protocol for the case of connected compact topological groups. This approach allows one to bypass and, in some cases, to completely eliminate the computational complexity of the exponentiation operation. Such an approach does not exist in the prior art.

SUMMARY OF INVENTION

[0024] Geometric key establishment system of the present invention allows for easy, secure, and rapid creation and distribution of encryption/decryption keys for major cryptosystems. The procedures of creation and distribution of keys are performed extremely rapidly and have very low computer memory requirements.

[0025] The present invention proposes a continuous version of Diffie-Hellman protocol. Based on this continuous Diffie-Hellman protocol, a method for public distribution of keys for encryption/decryption systems is implemented. An

embodiment of the method, while providing an extremely high security level, is several orders of magnitude faster than existing key distribution systems.

[0026] The key creation process of the system hereof uses the operation of linear combination with integer coefficients of irrational numbers and the operation of taking fractional parts of real numbers. In more advanced implementations the operation of taking fractional parts can be replaced by the exponentiation from the compact Lie algebra into the corresponding compact Lie group.

[0027] The system of the present invention constructs encryption/decryption keys on the fly out of a publicly chosen n-tuple g of irrational numbers and a pair of secret integer $n \times n$ matrices A and B, where the first integer matrix A is generated by the first communicating party and the second integer matrix B – by the second, and the matrices commute, i.e., A·B = B·A. Absolute values of matrix coefficients of these matrices are bounded by a publicly available constant 10^N that may be arbitrarily big. Thus the keys created and distributed by the system hereof can be of any given in advance size. The present invention combines the idea of Diffie-Hellman protocol of key distribution with the idea of the geometric cryptosystem devel-

oped in the U.S. Patent Application No*10/605,935*entitled GEOMETRY-BASED SYMMETRIC CRYPTOSYSTEM METHOD by the authors Arkady Berenstein and Leon Chernyak.

[0028] The security of the system of the present invention is based on the following well-known paradigm from Number Theory. Let β_1, β_2, ... be a sequence of irrational numbers (or more generally, of irrational elements of a compact Lie group) and let γ be an irrational number computed with the precision of K decimal places. Then any algorithm that recognizes γ as an element of the sequence β_1, β_2, ... and identifies the index n such that $\gamma = \beta_n$ must work at least $C \cdot 10^K$ units of time where C is an a priori given constant.

Brief Description of Drawings

[0029] FIG. 1 is a block diagram of the mathematical apparatus that can be used in practicing embodiments of the invention.

[0030] FIG. 2 is a flow diagram of the geometric key establishment system which shows generation of commuting matrices with integer coefficients; when taken with the subsidiary flow diagrams referred to therein, can be used in implementing embodiments of the invention.

[0031] FIG. 3 is a flow diagram of the geometric key establish-

ment system which shows the exponentiation of n-tuples of group elements into matrix powers; when taken with the subsidiary flow diagrams referred to therein, can be used in implementing embodiments of the invention.

[0032] FIG. 4 is a flow diagram of the geometric key establishment system which shows the fractional multiplication of n-tuples of real numbers by integer $n \times n$ matrices; when taken with the subsidiary flow diagrams referred to therein, can be used in implementing embodiments of the invention.

[0033] FIG. 5 is a block diagram of the geometric key establishment system that can be used in practicing n-dimensional embodiments of the invention.

[0034] FIG. 6 is a block diagram of the geometric key establishment system that can be used in practicing one-dimensional embodiments of the invention.

[0035] FIG. 7 is a block diagram of the geometric key establishment system that can be used in practicing preferred n-dimensional embodiments of the invention in the case when the group operation consists of taking the fractional part of sum of real numbers.

[0036] geometric key establishment system the is a block diagram of FIG. 8that can be used in practicing preferred

one-dimensional embodiments of the invention in the case when the group operation consists of taking the fractional part of sum of real numbers.

Detailed Description

[0037] The key creation and distribution techniques of an embodiment of the geometric key establishment system hereof are based on the operation of multiplication of real numbers by integers and the operation of evaluating fractional parts of real numbers. More specifically, the n-dimensional embodiment of the system hereof is based on the operation of multiplication of real vectors by integer matrices and on the operation of evaluating fractional parts of coordinates of the vectors.

[0038] In more advanced implementations the operation of evaluating fractional parts can be replaced by the exponentiation from the compact Lie algebra into the corresponding compact Lie group.

[0039] A preferred exemplary embodiment of such an apparatus is depicted with block diagram in FIG. 1, and is described as follows.

[0040] Let G be a compact connected group whose law of composition

[0041] $G \times G \rightarrow G$

[0042] is feasibly computable. There are among such groups the special orthogonal group, the unitary group and their closed connected subgroups. The block 101 generates such groups. Since each such group has uncountably many elements, the block 102 selects an element g of G essentially at random. The block 103 generates a n-tuple $g = (g_1, g_2, \ldots, g_n)$ of pairwise commuting elements g_1, $g_2, \ldots, g_n$ of G. This generator may proceed by choosing a commutative subgroup of G and then selecting elements $g_1, g_2, \ldots, g_n$ from this subgroup. Alternatively, the group generator 101 can start with choosing a commutative group G. The block 104 is designed for independent generation of commuting integer matrices, which procedure is depicted in more details in FIG. 2. The block 105 is designed for raising each n-tuple $g = (g_1, g_2, \ldots, g_n)$ into an integer matrix power, which procedure is depicted in more details in FIG. 3. The block 106 rounds each element g of the group G to the nearest element [g] of G. This procedure is depicted in more details in subsequent flow diagrams of FIG. 7 and FIG. 8, where, as a preferred embodiment of the invention hereof, the group operation of G consists of taking the fractional part of sum of real numbers. The block 107 applies the procedure of rounding of

the block 106 to each coordinate of a given n-tuple $g = (g_1, g_2, \ldots, g_n)$.

[0043] FIG. 2 illustrates a basic procedure of generation of commuting $n \times n$ matrices A and B independently by the first and the second communicating parties.

[0044] In the block 201 a public $n \times n$ matrix S is selected.

[0045] In the block 202 the first communicating party chooses at random secret integers $a_0, a_1, \ldots, a_{n-1}$, and in the block 204 creates a matrix A according to the formula:

[0046] $A = a_0 \cdot I + a_1 \cdot S + a_2 \cdot S^2 + \ldots + a_{n-1} \cdot S^{n-1}$.

[0047] In a similar manner and independently, in the block 203 the second communicating party chooses at random secret integers $b_0, b_1, \ldots, b_{n-1}$, and in the block 205 creates a matrix B according to the formula:

[0048] $B = b_0 \cdot I + b_1 \cdot S + b_2 \cdot S^2 + \ldots + b_{n-1} \cdot S^{n-1}$.

[0049] By the design, the matrices A and B commute: $A \cdot B = B \cdot A$.

[0050] FIG. 3 represents a basic procedure of raising a n-tuple g into the A-th power, where A is an $n \times n$ matrix.

[0051] In the block 301 an n-tuple $g = (g_1, g_2, \ldots, g_n)$ of elements of the group G is generated.

[0052] Independently, in the block 302 an $n \times n$ matrix A is generated.

[0053] And, in the block 303 the power g^A is computed according to the formula:

[0054] $g^A=(y_1, y_2,\ldots,y_n)$,

[0055] where

[0056] $y_j=g_1^{A1,j}\cdot g_2^{A2,j}\cdot\ldots\cdot g_n^{An,j}$

[0057] for j = 1, 2, ..., n, where A_{ij} is the (i,j)-th matrix coefficient of A.

[0058] FIG. 4 represents a basic procedure of implementing the routine of FIG. 3 in the case when the group operation consists of taking the fractional part of sum of real numbers.

[0059] In the block 401 an n-dimensional real vector $g = (g_1, g_2,\ldots, g_n)$ is generated.

[0060] Independently, in the block 402 an $n\times n$ matrix A is generated.

[0061] And, in the block 403 the fractional product $\{g\cdot A\}$ is computed according to the formula:

[0062] $\{g\cdot A\}=(y_1, y_2,\ldots,y_n)$,

[0063] where

[0064] $y_j=\{g_1A_{1,j} + g_2A_{2,j} +\ldots+ g_nA_{n,j}\}$

[0065] for j = 1, 2, ..., n, where A_{ij} is the (i,j)-th matrix coefficient

of A, and where $\{z\}$ stands for the fractional part of the real number z (for example, {1.7}=0.7, {-1.7}=0.3).

[0066] FIG. 5 illustrates creation, establishment, and distribution of a geometric key in an n-dimensional embodiment of the system of the present invention. It refers to the routines illustrated by other referenced flow diagrams (FIG. 1, FIG. 2, FIG. 3) which describe features in accordance with an embodiment of the invention.

[0067] The block 501 represents generation of the public compact connected commutative topological group G and a choosing at random a public n-tuple $g = (g_1, g_2, \ldots, g_n)$ of elements of G. A public $n \times n$ matrix S is also chosen in this block. Both, g and S are to be used by both communicating parties.

[0068] The block 502 represents the routine that can be used by the first communicating party for generating a private matrix A according to the routine of FIG. 2.

[0069] Similarly, the block 503 represents the routine that can be used by the second communicating party for generating a private matrix B according to the routine of FIG. 2.

[0070] The block 504 represents computation (by the first communicating party) of the n-tuple g^A according to the routine of FIG. 3, and rounding g^A to the nearest n-tuple [g

]. The rounded n-tuple $[g^A]$ is then transmitted over an open (public) channel to the second communicating party.

[0071] Similarly, the block 505 represents computation (by the first communicating party) of the n-tuple g^B according to the routine of FIG. 3, and rounding g^B to the nearest n-tuple $[g^B]$. The rounded n-tuple $[g^B]$ is then transmitted over an open (public) channel to the first communicating party.

[0072] The block 506 represents the routine that can be used by the second communicating party for generating the n-tuple $[g^A]^B$ (according to the routine of FIG. 3) and rounding it to the nearest n-tuple $[[g^A]^B]$.

[0073] Similarly, the block 507 represents the routine that can be used by the first communicating party for generating the n-tuple $[g^B]^A$ (according to the routine of FIG. 3) and rounding it to the nearest n-tuple $[[g^B]^A]$.

[0074] By the design, the n-tuples $[[g^A]^B]$ and $[[g^B]^A]$ are equal, and thus comprise the common secret geometric key in possession of both communicating parties.

[0075] FIG. 6 illustrates creation, establishment, and distribution of a geometric key in a one-dimensional embodiment of the system of the present invention. It refers to the routines illustrated by other referenced flow diagrams which

describe features in accordance with an embodiment of the invention.

[0076] The block 601 represents generation of the public compact connected topological group G and a choosing at random a public element g of G, which g is to be used by both communicating parties.

[0077] The block 602 represents the routine that can be used by the first communicating party for generating a private integer a, computing the a-thpower g^a of g, and rounding g^a to the nearest element $[g^a]$ in G. This rounded element $[g^a]$ is then transmitted over an open (public) channel to the second communicating party.

[0078] Similarly, the block 603 represents the routine that can be used by the second communicating party for generating a private integer b, computing the b-thpower g^b of g, and rounding g^b to the nearest element $[g^b]$ in G. This rounded element $[g^b]$ is then transmitted over an open (public) channel to the second communicating party.

[0079] The block 604 represents the routine that can be used by the second communicating party for generating the element $[g^a]^b$ and rounding it to the nearest element $[[g^a]^b]$.

[0080] Similarly, the block 605 represents the routine that can be used by the first communicating party for generating the

element $[g^b]^a$ and rounding it to the nearest element $[[g^b]^a]$.

[0081] By the design, the elements $[g^a]^b$ and $[g^b]^a$ are equal in G, and thus comprise the common secret geometric key in possession of both communicating parties.

[0082] FIG. 7 represents creation, establishment, and distribution of a key in an embodiment of the geometric key establishment system of present invention.

[0083] First, public natural numbers D, N, K are generated in the block 701. Next, a public n-dimensional decimal vector $g = (g_1, g_2, \ldots, g_n)$ having D+2N+K after dot is generated in the same block 701. And an integer $n \times n$ matrix S is chosen.

[0084] Then in the block 702 private integers $a_0, a_1, \ldots, a_{n-1}$ (each between -10^N and 10^N) are generated at random; next, a private matrix A is generated according to routine of FIG. 2.

[0085] In a similar manner, in the block 703 private integers $b_0, b_1, \ldots, b_{n-1}$ (each between -10^N and 10^N) are generated at random; next, a private matrix B is generated according to routine of FIG. 2.

[0086] In the block 704 the fractional vector $\{g \bullet A\}$ is computed according to the routine of FIG. 4. Next, each coordinate

of the resulted vector is rounded to D+N+K decimal places. The rounded fractional vector $\{g \bullet A\}$is then transmitted to the second communicating party.

[0087] In a similar manner, in the block 705 the fractional vector $\{g \bullet B\}$ is computed according to the routine of FIG. 4. First, the vector g is multiplied by the matrixB. Next, each coordinate of the resulted vector is rounded to D+N+K decimal places. The rounded fractional vector $\{g \bullet B\}$is then transmitted to the second communicating party.

[0088] The block 706 represents the routine that can be used by the second communicating party for computing the fractional vector $\{\{g \bullet A\} \bullet B\}$. The loop 708 is used in the case when the vector $\{\{g \bullet A\} \bullet B\}$ is not (K,D)-consistent (that is, in the case when the sequence of the digits d_{K+1}, d_{K+2}, ... d_{K+D} of at least one coordinate of the vector $\{\{g \bullet A\} \bullet B\}$ is either 0, 0, ..., 0 or 9, 9, ...,9.) The loop 708 is continued until the vector $\{\{g \bullet A\} \bullet B\}$ becomes (K,D)-consistent. [The probability of a vector $\{\{g \bullet A\} \bullet B\}$ to be not (K,D)-consistent is extremely low. Namely, this probability is measured as at most $1-(1-2 \cdot 10^{-D})^n$. The probability of the need for the second run of the loop 708 is measured as at most $(1-(1-2 \cdot 10^{-D})^n)^2$]. The block 710 is then entered, this block represents the generation of a vector γ which is the

rounding of the (K, D)-consistent vector {{g•A}•B} to K decimal places.

[0089] In a similar manner the block 707 represents the routine that can be used by the first communicating party for computing the fractional vector {{g•B}•A}. The loop 709 is used in the case when the vector {{g•B}•A} is not (K,D)-consistent (that is, in the case when the sequence of the digits d_{K+1}, d_{K+2}, ... d_{K+D} of at least one coordinate of the vector {{g•B}•A} is either 0, 0, ..., 0 or 9, 9, ..., 9.) The loop 709 is continued until the vector {{g•B}•A} becomes (K,D)-consistent. [The probability of a vector {{g•B}•A} to be not (K,D)-consistent is extremely low. Namely, this probability is measured as at most $1-(1-2\cdot10^{-D})^n$. The probability of the need for the second run of the loop 709 is measured as at most $(1-(1-2\cdot10^{-D})^n)^2$]. The block 711 is then entered, this block represents the generation of a vector γ' which is the rounding of the (K, D)-consistent vector {{g•B}•A} to K decimal places.

[0090] By the design, the vectors γ and γ' are equal, and thus comprise the common secret key in possession of both communicating parties.

[0091] FIG. 8 represents creation, establishment, and distribution of a key in an embodiment of the geometric key estab-

lishment system of present invention.

[0092] First, a public real number α and public natural numbers D, N, K are generated in the block 801.

[0093] Then in the block 802 a private integer a (between -10^N and 10^N) is generated at random, and the number $\{\alpha a\}$is computed and rounded to D+N+K decimal places by the first communicating party. The rounded number $\{\alpha a\}$is then transmitted to the second communicating party.

[0094] In a similar manner, in the block 803 a private integer b (between -10^N and 10^N) is generated at random, and the number $\{\alpha b\}$is computed and rounded to D+N+K decimal places by the second communicating party. The rounded number $\{\alpha b\}$is then transmitted to the first communicating party.

[0095] The block 804 represents the routine that can be used by the second communicating party for computing the number $\{\{\alpha a\}b\}$. The loop 806 is used in the case when the number $\{\{\alpha a\}b\}$ is not (K, D)-consistent (that is, in the case when the sequence of the digits $d_{K+1}, d_{K+2}, \ldots, d_{K+D}$ of the number $\{\{\alpha a\}b\}$ is either 0, 0, ...,0 or 9, 9, ...,9). The loop 806 is continued until the number $\{\{\alpha a\}b\}$ becomes (K, D)-consistent. [The probability of a number $\{\{\alpha a\}b\}$ to be not (K,D)-consistent is extremely low. Namely, this

probability is measured as at most $2 \cdot 10^{-D}$. The probability of the need for the second run of the loop 806 is measured as at most $(2 \cdot 10^{-D})^2$]. The block 808 is then entered, this block represents the generation of a number γ which is the rounding of the (K, D)-consistent number {{α *a*}*b*} to K decimal places.

[0096] In a similar manner block 805 represents the routine that can be used by the first communicating party for computing the number {{α*b*}*a*}. The loop 807 is used in the case when the number {{α*b*}*a*} is not (K,D)-consistent (that is, in the case when the sequence of the digits d_{K+1}, d_{K+2}, ... , d_{K+D} of the number {{α*b*}*a*} is either 0, 0, ...,0 or 9, 9, ..., 9). The loop 805 is continued until the number {{α*a*}*b*} becomes (K,D)-consistent. [The probability of a number {{α*b*} *a*} to be not (K,D)-consistent is extremely low. Namely, this probability is measured as at most $2 \cdot 10^{-D}$. The probability of the need for the second run of the loop 807 is measured as at most $(2 \cdot 10^{-D})^2$]. The block 809 is then entered, this block represents the generation of a number γ′ which is the rounding of the (K,D)-consistent number {{α *b*}*a*} to K decimal places.

[0097] By the design, the numbers γ and γ′ are equal, and thus comprise the common secret key in possession of both

communicating parties.

[0098]

[0099] The security of the system of the present invention comes from the built-in geometric density of certain sequences of irrational numbers in the semi-open interval [0, 1) of the real line. In other words, security of the proposed system is guaranteed by the obvious mathematical fact that there is no any a priori known general distribution pattern for members of certain sequences of irrational numbers.

[0100] More precisely, let $\beta_1, \beta_2, \ldots$ be a sequence of irrational numbers (or more generally, of irrational elements of a compact Lie group) and let γ be an irrational number computed with the precision of K decimal places. Then any algorithm that recognizes γas an element of the sequence $\beta_1, \beta_2, \ldots$ and identifies the index n such that $\gamma = \beta_n$ must work at least $C \cdot 10^K$ units of time where C is an a priori given constant.

[0101] Apparently, approaches that are the closest to the present invention are developed in U.S. Pat. No 5,696,826entitledMETHOD AND APPARATUS FOR ENCRYPTING AND DECRYPTING INFORMATION USING A DIGITAL CHAOS SIGNAL by Gao, in U.S. Pat. No 6,493,449 entitledMETHOD AND APPARATUS FOR CRYPTOGRAPHICALLY

SECURE ALGEBRAIC KEY ESTABLISHMENT PROTOCOLS BASED ON MONOIDS by Anshel et al, and in U.S. Patent Application No10/605,935entitled GEOMETRY-BASED SYMMETRIC CRYPTOSYSTEM METHOD by Berenstein and Chernyak.

[0102] The idea of using fractional parts of multiples of given irrational numbers is not new in cryptography. This idea is used to obtain a uniform distribution of numbers in the unit interval. It was used, for example, in the patent by Gao. However, this is perhaps the only similarity between these previous works and the system of the present invention. In the system hereof, fractional parts of multiples of given irrational numbers are never used for obtaining a uniform distribution of numbers, but rather for creation of a deterministic (non-random) keys.

[0103] The idea of using infinite groups for key establishment an exchange is relatively new. It is presented in the patent by Anshel et al. However, the present invention is the first where continuous, topological groups are used for key establishment and exchange. In patent application by Berenstein and Chernyak the geometric continuity is utilized for constructing private encryption systems.

[0104] An embodiment of the system hereof deals with a publicly

chosen real number α and a pair of secret integers a and b, where the first integer a is generated by the first communicating party and the second integer b - by the second communicating party. Absolute value of each of these integers is bounded by a publicly available constant 10^N that may be arbitrarily big. Thus the keys created and distributed by the system hereof can be of any given in advance size. The present invention combines the idea of Diffie-Hellman protocol of key establishment with the idea of the geometric cryptosystem developed in the patent application No 10/605,935 by the authors Arkady Berenstein and Leon Chernyak.

[0105] In this embodiment the real number αcanbe chosen essentially at random from the infinite set of known real numbers. This choice can include such numbers as, for example, $\sqrt{m}$, where m is any natural number that is not a complete square, or, more generally, αcan be any irrational real root of an algebraic equation with integer coefficients. Also α can be chosen, for example, as π^n or e^n, where n is any natural number, or, more generally, α can be any polynomial with integer coefficients evaluated at a given transcendental number. Another possible source of irrational numbers may include, for example, sin(n), cos(

), ln(n), where n is any natural number; or, more generally, α can be any transcendental function evaluated at a given natural number.

[0106] Let $\{x\}$ be the fractional part of a real number x. By definition, for each real number x, the fractional part $\{x\}$ is given by:

[0107] $\{x\} = x - [x]$,

[0108] where $[x]$ is the integer part of x, that is, $[x]$ is the greatest integer that is less or equal x. If the numbers a and b are integers having at most N decimal digits each (that is, $|a| < 10^N$ and $|b| < 10^N$) and each of the numbers $\{\alpha a\}$ and $\{\alpha b\}$ is rounded to D+N+K decimal places after dot (where D, N, and K are natural numbers each greater than 1), then the created and distributed key, which is $\{\alpha ab\}$, will have K correct decimal places after the dot. These K correct digits serve as the encryption/decryption key of major cryptosystems.

[0109] The security of the system of the present invention is based on the following well-known paradigm from Number Theory. Let β_1, β_2, ...be a sequence of irrational numbers (or more generally, of irrational elements of a compact Lie group) and let γ be an irrational number computed with the precision of K decimal places. Then any al-

gorithm that recognizes γas an element of the sequence $\beta_1, \beta_2, \ldots$and identifies the index n such that $\gamma = \beta_n$ must work at least $C \cdot 10^K$ units of time where C is an a priori given constant.

[0110] In particular, the security of the system hereof is based on the fact that there cannot be any a priori known general distribution pattern of fractional parts of multiples of each taken at random irrational number α. Therefore, the security level of the system hereof can be measured as a number of operations needed for reconstruction of the number a out of a given fractional number $\{\alpha a\}$ calculated with the precision of D+N+K decimal places. The above implies that the only way to reconstruct the number a out of a given fractional number $\{\alpha a\}$ is to list all possible numbers $\{\alpha L\}$, where L is any integer between -10^N and 10^N. The number of such numbers L is $2 \cdot 10^N - 1$.

[0111] For a cryptanalyst, the only alternative to listing all possible numbers a is to list all possible shared K-digits keys. The number of such keys is 10^K. Therefore, the security level of the system hereof can be measured as the minimum of the two numbers $2 \cdot 10^N - 1$ and 10^K.

[0112] The processor time required for creation and distribution of one geometric key is at most quadratic in N and K, or,

more precisely, is at most N(2D + 3N + 2K) units of processor time. This speed is several orders of magnitude higher than in existing key establishment systems.

[0113] In creating geometric key establishment system in accordance with an embodiment hereof, a first step is to choose publicly available parameters of the system: a real number α and natural numbers D, N, K, each greater than 1, where D stand for the size of the *error control buffer*, N stands for the maximum number of decimal places in each secret parameter a and b, and K stands for the key length.

[0114] An embodiment of the geometric key establishment system hereof relies on the concept of (K, D)-consistent numbers. An infinite decimal fraction $\delta = 0.\, d_1\, d_2\, d_3 \ldots$ is said to be (K, D)-consistent if the sequence of the digits $d_{K+1}, d_{K+2}, \ldots, d_{K+D}$ is neither 0, 0, ..., 0 nor 9, 9, ..., 9.

[0115] To implement the key creation and key distribution of this example, the first communicating party, call it Alice, chooses a secret integer a between -10^N and 10^N (i.e., a has at most N decimal places), calculates the number β, which is the fractional part $\{\alpha a\}$ rounded to D+N+K decimal places, and sends so calculated rounding βof $\{\alpha a\}$ to the second the first communicating party, call it Bob. [It is

assumed in this example that Alice and Bob share the publicly available parameters αand D, N, K]. Simultaneously and independently Bob chooses a secret integer b between -10^N and 10^N (i.e., b has at most N decimal places), calculates the number β', which is the fractional part {αb} rounded to D+N+K decimal places, and sends so calculated rounding β' of {αb} to Alice. Upon receiving β from Alice, Bob multiplies β by b, computes the fractional part {βb} with the precision of K + D decimal places after the dot. If {βb} is (K, D)-consistent, Bob computes the number γ that is the rounding of {βb} to the K digits after the decimal dot. This number γis the geometric key in possession of Bob. Upon receiving β' from Bob, Alice multiplies β' by a, computes the fractional part {β'a} with the precision of K + D decimal places after the dot. If {β'a} is (K, D)-consistent, Alice computes the number γ' that is the rounding of {β'a} to the K digits after the decimal dot. Then Alice computes the number γ' that is the rounding of {β'a} to the K digits after the decimal dot. This number γ' is the geometric key in possession of Alice. In this case (which is the general case), the geometric key γis equal to the geometric key γ'. In those (extremely rare) cases when {βb} is not (K, D)-consistent, the geometric key has to be

redistributed because otherwise it may happen that $\gamma \neq \gamma'$. In order to avoid such a situation, Alice and Bob choose new secret numbers a_1 and b_1 respectively (while keeping the same α and D, N, K) and repeat the above steps until they get a new geometric key $\gamma_1 = \gamma'_1$ (provided that the new number $\{\beta_1 b_1\}$ is (K, D)-consistent).

[0116] The probability of the need for such redistribution is extremely low and is measured as at most $2 \cdot 10^{-D}$. The probability of the need for the second key distribution is measured as at most $(2 \cdot 10^{-D})^2$.

[0117] The embodiment of the system hereof is based on the following mathematical argument.

[0118] The definition of the fractional part $\{x\}$ of x implies that $\{x\}$ always belongs to the semi-open interval [0, 1), and that

[0119] $$\{x + c\} = \{x\}$$

[0120] for any integer c. In its turn this implies that

[0121] $$\{\{x\}d\} = \{xd\}$$

[0122] for any integer d. Therefore,

[0123] $$\{\{\alpha a\}b\} = \{\alpha ab\} = \{\alpha ba\} = \{\{\alpha b\}a\}.$$

[0124] Since $-10^N < a < 10^N$, and $-10^N < b < 10^N$; and both $\{\alpha a\}$ and $\{\alpha b\}$ are computed with D+N+K correct decimal

places after dot, it is asserted that the left hand side $\{\{\alpha a\} b\}$ and the right hand side $\{\{\alpha b\}a\}$ are equal in the first K decimal places after dot if $\{\alpha a\}$ and $\{\alpha b\}$ are both (K, D)-consistent. In order to prove the assertion, the following notation is introduced. Let $\{\alpha a\}$ be rounded to D+N+K correct decimal places, i.e., to the number

[0125] $$\beta = \{\alpha a\} + \theta \cdot 10^{-(D+N+K)},$$

[0126] where $|\theta| < 0.5$, and let $\{\alpha b\}$ be also rounded to N + D + K correct decimal places, i.e., to the number

[0127] $$\beta' = \{\alpha b\} + \theta' \cdot 10^{-(D+N+K)},$$

[0128] where $|\theta'| < 0.5$. Then $\{\{\alpha a\}b\}$ is calculated as $\{\beta b\}$ and $\{\{\alpha b\}a\}$ is calculated as $\{\beta' b\}$. Furthermore,

[0129] $$\{\beta b\} = \{(\{\alpha a\} + \theta \cdot 10^{-(D+N+K)})b\} = \{\{\alpha a\}b + \theta \cdot 10^{-(D+N+K)} \cdot b\} =$$

[0130] $$= \{\{\alpha a\}b + \theta_1 \cdot 10^{-D-K}\} = \{\{\{\alpha a\}b\} + \theta_1 \cdot 10^{-D-K}\} = \{\{\alpha ab\} + \theta_1 \cdot 10^{-D-K}\},$$

[0131] where θ_1 is some number such that $|\theta_1| < 0.5$.

[0132] Similarly

[0133] $$\{\beta' a\} = \{(\{\alpha b\} + \theta' \cdot 10^{-(D+N+K)})a\} = \{\{\alpha b\}a + \theta' \cdot 10^{-(D+N+K)} \cdot a\} =$$

[0134] $$= \{\{\alpha b\}a + \theta'_1 \cdot 10^{-D-K}\} = \{\{\{\alpha b\}a\} + \theta'_1 \cdot 10^{-D-K}\} = \{\{\alpha ba\} + \theta'_1 \cdot 10^{-D-K}\},$$

[0135] where θ'_1 is some number such that $|\theta'_1| < 0.5$.

[0136] Let γ be the rounding of {βb} to K decimal places after dot and let γ' be rounding of {β'a} to K decimal places after dot. The above calculation of {βb} and {β'a} ensures that, if γ≠γ', then necessarily one of these numbers, say {βb}, has all digits equal 9 at each i-th decimal place after dot, when i = K + 1, K + 2, ... , K + D, and, at the same time, the second of these numbers, i.e., {β'a}, has digits equal 0 at each i-th decimal place after dot, when i = K + 1, K + 2, ... , K + D. In other words, γ≠γ' implies that both {βb} and {β'a} are not (K, D)-consistent. Therefore, if {βb} is (K, D)-consistent, γ= γ'. Similarly, γ= γ' if {β'a} is (K, D)-consistent. This proves the assertion.

[0137] In creating geometric key establishment system in accordance with an embodiment hereof (and with the following small numbers for ease of illustration), a first step is to choose publicly available parameters of the system: an real number α and integer parameters D, N, K greater than 1 each. Take, for example, α= $\sqrt{2}$, N=K=8, D=2. Next, suppose that Alice chooses the number a = 48 176 925. Alice calculates the number {αa} with the precision D+N+K = 18 by β= {αa} = {$\sqrt{2}$·48 176 925} = 0.72843142218399O298 and sends this number β to Bob.

Suppose that at the same time Bob chooses the number b = 19082791. Bob calculates the number $\{\alpha b\}$ with the precision D+N+K = 18 by $\beta' = \{\alpha b\} = \{\sqrt{2}\cdot 19082791\} =$ 0.840131236839417426 and sends this number β' to Alice. Upon receiving the number βfrom Alice, Bob multiplies βby b, computes the fractional part $\{\beta b\}$ with the precision K + D = 10 decimal places after dot:

[0138] $\{\beta b\} = \{0.72843142218399 0298 \cdot 19082791\} =$ 0.5873698504.

[0139] Since this number is (K, D)-consistent, i.e., it has digits 0 and 4 at 9^{th} and 10^{th} places after dot, the first K = 8 digits of this number is the geometric key in possession of Bob:

[0140] γ= 0.58736985.

[0141] Upon receiving the number β' from Bob, Alice multiplies β' by a, computes the fractional part $\{\beta' a\}$ with the precision K + D = 10 decimal places after dot:

[0142] $\{\beta' a\} = \{0.840131236839417425 96 \cdot 48\ 176\ 925\} =$ 0.5873698504.

[0143] Since this number is (K, D)-consistent, i.e., it has digits 0 and 4 at 9^{th} and 10^{th} places after dot, the first K = 8 digits of this number is the geometric key in possession of Alice:

[0144] γ' = 0.58736985.

[0145] Thus, γ= γ' is the geometric key shared by Alice and Bob. This key can be used in any major symmetric cryptosystem.

[0146] In a further embodiment of the invention the real number α is replaced by the 2-dimensional real vector $g=(g_1, g_2)$ in order to further enhance the security level of the proposed system.

[0147] A 2-dimensional embodiment of the system hereof works with the semi-open unit square and integer 2×2 matrices A and B of the form:

[0148]
$$A = \begin{bmatrix} a_0 & -a_1 \\ a_1 & a_0 \end{bmatrix}$$

[0149] and

[0150]
$$B = \begin{bmatrix} b_0 & -b_1 \\ b_1 & b_0 \end{bmatrix}$$

[0151] where a_0, a_1, b_0, b_1 are arbitrary integers. This structure of A and B guarantees their commutation: A·B = B·A.

[0152] Absolute values of each integer a_0, a_1, b_0, b_1 are bounded by a publicly available constant 10^N that may be arbitrarily big. Thus the keys created and distributed by the system hereof can be of any given in advance size.

[0153] In this embodiment the vector $g=(g_1, g_2)$ has coordinates g_1 and g_2 which are arbitrary real numbers, that is, g is an arbitrary point of plane.

[0154] Let $\{x\}$ be the fractional part of a real number x. By definition, for each real number x, the fractional part $\{x\}$ is given by:

[0155] $\{x\}= x - [x]$,

[0156] where $[x]$ is the integer part of x, that is, $[x]$ is the greatest integer that is less or equal x.

[0157] If the numbers a_0, a_1 and b_0, b_1 are integers having at most N decimal digits each (that is, $|a_0| < 10^N$, $|a_1| < 10^N$ and $|b_0| < 10^N$, $|b_1| < 10^N$) and each coordinate of the vectors

[0158] $\{g\bullet A\}=(\{g_1 a_0 + g_2 a_1\},\{- g_1 a_1 + g_2 a_0\})$ and $\{g\bullet B\}=(\{g_1 b_0 + g_2 b_1\},\{- g_1 b_1 + g_2 b_0\})$

[0159] is rounded to D+N+K decimal places after dot (where D, N, and K are natural numbers each greater than 1), then

the created and distributed key, which is the vector {$g \bullet A \bullet B$}, in each of its coordinates will have K correct decimal places after the dot. These 2K correct digits serve as the encryption/decryption key of major cryptosystems.

[0160] The security of this two-dimensional embodiment is further enhanced even in comparison with the high security of the one-dimensional embodiment.

[0161] In creating geometric key establishment system in accordance with the 2-dimensional embodiment hereof, a first step is to choose publicly available parameters of the system: a real vector $g=(g_1, g_2)$ and natural numbers D, N, K, each greater than 1, where D stand for the size of the *error control buffer*, N stands for the maximum number of decimal places in each secret parameter a and b, and K stands for the key length.

[0162] This embodiment of the geometric key establishment system hereof relies on the concept of (K, D)-consistent vectors. An infinite decimal fraction $\delta = 0.d_1 d_2 d_3 \ldots$ is said to be (K, D)-consistent if the sequence of the digits d_{K+1}, d_{K+2}, ..., d_{K+D} is neither 0, 0, ..., 0 nor 9, 9, ..., 9. We say that a vector (x_1, x_2) is (K,D)-consistent both x_1 and x_2 are (K,D)-consistent numbers.

[0163] To implement the key creation and key distribution of this

example, the first communicating party, call it Alice, chooses a pair of secret integers (a_0, a_1) each between -10^N and 10^N (i.e., each of these integers has at most N decimal places). Then Alice calculates the vector (y_1, y_2), where y_1 is $\{g_1 a_0 + g_2 a_1\}$ rounded to D+N+K decimal places and y_2 is$\{-g_1 a_1 + g_2 a_0\}$ rounded to D+N+K decimal places; and sends so calculated vector (y_1, y_2) to the second communicating party, call it Bob. [It is assumed in this example that Alice and Bob share the publicly available parameters $g=(g_1, g_2)$ and D, N, K.]

[0164] Simultaneously and independently Bob chooses a pair of secret integers (b_0, b_1) each between -10^N and 10^N (i.e., each of these integers has at most N decimal places). Then Bob calculates the calculates the vector (z_1, z_2), where z_1 is $\{g_1 b_0 + g_2 b_1\}$ rounded to D+N+K decimal places and z_2 is$\{- g_1 b_1 + g_2 b_0\}$ rounded to D+N+K decimal places; and sends so calculated so calculated vector (z_1, z_2) to Alice.

[0165] Upon receiving the vector (y_1, y_2) from Alice, Bob calculates the vector (k_1, k_2) by the formula:

[0166] $(k_1, k_2)=(\{y_1 b_0 + y_2 b_1\}, \{- y_1 b_1 + y_2 b_0\})$.

[0167] If the vector (k_1, k_2) is (K, D)-consistent then Bob calculates the geometric key (s_1, s_2) by rounding each coordi-

nate of (k_1, k_2) to K decimal places. Otherwise, he restarts the protocol.

[0168] Upon receiving the vector (z_1, z_2) from Bob, Alice calculates the vector (k'_1, k'_2) by the formula:

[0169] $(k'_1, k'_2)=(\{z_1 a_0 + z_2 a_1\}, \{- z_1 a_1 + z_2 a_0\})$.

[0170] If the vector (k'_1, k'_2) is (K, D)-consistent then Alice calculates the geometric key (s'_1, s'_2) by rounding each coordinate of (k'_1, k'_2) to K decimal places. Otherwise, she restarts the protocol.

[0171] The mathematical argument presented below proves that the geometric key (s_1, s_2) in possession of Bob to the geometric key (s'_1, s'_2) in possession of Alice.

[0172] In those (extremely rare) cases when (k_1, k_2) is not (K, D)-consistent, the geometric key has to be redistributed because otherwise it may happen that $(s_1, s_2) \neq (s'_1, s'_2)$. In order to avoid such a situation, Alice and Bob choose new pairs of secret numbers (a'_0, a'_1) and (b'_0, b'_1) respectively (while keeping the same $g=(g_1, g_2)$ and D, N, K) and repeat the above steps until they get a new geometric key $(s_1, s_2) = (s'_1, s'_2)$ (provided that the new vector (k_1, k_2) is (K, D)-consistent).

[0173] The probability of the need for such redistribution is extremely low and is measured as at most $4 \cdot 10^{-D}$. The prob-

ability of the need for the second key distribution is measured as at most $(4\cdot 10^{-D})^2$.

[0174] The embodiment of the system hereof is based on the following mathematical argument.

[0175] *Proposition*. Let be $P=(P_1, P_2,..., P_n)$, $Q=(Q_1, Q_2,..., Q_n)$, and $L=(L_1, L_2,..., L_n)$ be n-tuples of natural numbers. Let α and β be n×n matrices with natural coefficients such that:

[0176] $Q^{-1}\cdot\alpha\leq L^{-1}$, $P^{-1}\cdot\beta\leq L^{-1}$.

[0177] Then for any real vector $g = (g_1, g_2,...,g_n)$ any $n\times n$ matrices A and B with integer coefficients such that A·B = B·A and

[0178] $|A_{ij}|<\alpha_{ij}$, $|B_{ij}|<\beta_{ij}$

[0179] (for all i=1,2,.., n, j=1,2,..,n) one has: either at least one coordinate of $[\{([\{g\cdot A\}]_P)\cdot B\}]_L$ equals 0,or at least one coordinate of$[\{([\{g\cdot B\}]_Q)\cdot A\}]_L$ equals 0, or

[0180] $\{([\{g\cdot A\}]_P)\cdot B\}-\{([\{g\cdot B\}]_Q)\cdot A\}=\theta\cdot L^{-1}$,

[0181] *Proof*. By definition, one has:

[0182] $[\{g\cdot A\}]_P=\{g\cdot A\}+\theta_1\cdot P^{-1}$, $[\{g\cdot B\}]_Q=\{g\cdot B\}+\theta_2\cdot Q^{-1}$,

[0183] where $-½\leq\theta_1\leq½$ and $-½\leq\theta_2\leq½$. Therefore,

[0184] $([\{g\cdot A\}]_P)\cdot B=(\{g\cdot A\}+\theta_1\cdot P^{-1})\cdot B=\{g\cdot A\}\cdot B+\theta_1\cdot P^{-1}\cdot B=\{g\cdot A\}\cdot B+E_1$,

[0185] where $E_1=\theta_1\cdot P^{-1}\cdot B$.

[0186] Similarly,

[0187] $([\{g\cdot B\}]_Q)\cdot A=(\{g\cdot B\}+\theta_2\cdot Q^{-1})\cdot A=\{g\cdot B\}\cdot A+\theta_2\cdot Q^{-1}\cdot A=\{g\cdot B\}\cdot A+E_2$,

[0188] where $E_2=\theta_2\cdot Q^{-1}\cdot A$.

[0189] By the assumptions, one has:

[0190] $|E_1|=|\theta_1\cdot P^{-1}\cdot B|\le 1/2\cdot|P^{-1}\cdot B|<1/2\cdot P^{-1}\cdot\beta\le 1/2\cdot L^{-1}$

[0191] and

[0192] $|E_2|=|\theta_2\cdot Q^{-1}\cdot A|\le 1/2\cdot|Q^{-1}\cdot A|<1/2\cdot Q^{-1}\cdot\alpha\le 1/2\cdot L^{-1}$.

[0193] In its turn, this implies that either $|([\{g\cdot A\}]_P)\cdot B|$ is not greater than L^{-1} or:

[0194] $\{([\{g\cdot A\}]_P)\cdot B\}=\{\{g\cdot A\}\cdot B+E_1\}=\{\{g\cdot A\}\cdot B\}+E_1=\{g\cdot A\cdot B\}+E_1$.

[0195] Similarly, this implies that either $|([\{g\cdot B\}]_Q)\cdot A|$ is not greater than L^{-1} or:

[0196] $\{([\{g\cdot B\}]_Q)\cdot A\}=\{\{g\cdot B\}\cdot A+E_2\}=\{\{g\cdot B\}\cdot A\}+E_2=\{g\cdot B\cdot A\}+E_2$.

[0197] Since $A\cdot B=B\cdot A$, one has:

[0198] $\{([\{g\cdot A\}]_P)\cdot B\}-\{([\{g\cdot B\}]_Q)\cdot A\}=E_1-E_2=\theta\cdot L^{-1}$,

[0199] where $-1<\theta<1$. □

[0200] We say that a vector $x=(x_1,x_2,\ldots,x_n)$ is (K, D)-consistent if:

[0201] $(-c, -c, \ldots, -c) \leq x-[x]_K \leq (c, c, \ldots, c)$,

[0202] where $c=1/2-1/(2D)$.

[0203] *Corollary*. In the notation of the Proposition, if $L=D\cdot K$ and one the vectors $\{([\{g\cdot A\}]_P)\cdot B\}$ and $\{([\{g\cdot B\}]_Q)\cdot A\}$ is (K, D)-consistent then

[0204] $[([\{g\cdot A\}]_P)\cdot B]_K = [([\{g\cdot B\}]_Q)\cdot A]_K$.

[0205] For the 2-dimensional embodiment of the system hereof the Corollary is applied with $n=2$, $K=(K,K)$. Therefore, the Corollary guarantees that $(s_1, s_2) = (s'_1, s'_2)$ in the protocol.

[0206] In creating a geometric key establishment system in accordance with the two-dimensional embodiment hereof (and with the following small numbers for ease of illustration), a first step is to choose publicly available parameters of the system: a vector $g=(g_1, g_2)$ and integer parameters D, N, K greater than 1 each. Take, for example, $g_1 = \sqrt{2}$, $g_2 = \sqrt{3}$, N = K = 8, D = 2. Next, suppose that Alice chooses a pair of secret integers $(a_0, a_1) = (48176925, 18034725)$. Alice calculates the vector

[0207] $(y_1, y_2)=(\{g_1a_0 + g_2a_1\}, \{- g_1a_1+ g_2a_0\})$

[0208] each coordinate of which rounded to D+N+K = 18 decimal places:

[0209] (y_1, y_2)=({ √2·48176925 + √3·18034725},
{-√2·18034725+ √3·48176925})=

[0210] ({68132460.728431422183990297539596+31237060.0
0053262054751177472131 4},
{-25504952.688669116604000035676723+83444881.8
52435233704474767836253})

[0211] =(0.72896404273150207 2, 0.1637661171004747 32)

[0212] and sends this vector (y_1, y_2) to Bob. Suppose that at the same time Bob a pair of secret integers (b_0, b_1) = (19082792, 27045821). Alice calculates the vector

[0213] (z_1, z_2)=({$g_1b_0 + g_2b_1$}, {$- g_1b_1 + g_2b_0$ })

[0214] each coordinate of which rounded to D+N+K = 18 decimal places:

[0215] (z_1, z_2)= ({ √2·19082792 + √3·27045821},
{-√2·27045821+ √3·19082792})=
({26987143.254344799212512475172839+
46844736.104413300451707772339473},
{-38248566.863715063905876737732694+
33052365.294268911065907204826118})=

[0216] =(0.358758099664220248, 0.43055384716003046 7)

[0217] and sends this vector (z_1, z_2) to Alice. Upon receiving the vector (y_1, y_2) from Alice, Bob calculates the vector $(k_1, k$

) by the formula:

[0218] $(k_1, k_2)=(\{y_1 b_0 + y_2 b_1\}, \{- y_1 b_1 + y_2 b_0\})$

[0219] with the precision K + D = 10 decimal places after dot:

[0220] $(k_1, k_2)=(\{0.72896404273150207 2 \cdot 19082792+0.1637661171 00474732 \cdot 27045821\}, \{- 0.72896404273150207 2 \cdot 27045821+ 0.1637661171 00474732 \cdot 19082792\}) =$

[0221] $=(\{13910669.2029243658875450244429189.088964478616694972\},\{-19715431.01515255610044111253114.749276002412011744\})$

[0222] $=(0.2918888445, 0.7341234463)$

[0223] Since this vector is (K,K, D)-consistent (i.e., its first coordinate has digits 4 and 5 at 9^{th} and 10^{th} places after dot, and its second coordinate has digits 6 and 3 at 9^{th} and 10^{th} places after the dot), the vector (k_1, k_2), being rounded to the first K = 8 digits of each coordinate, constitutes the geometric key in possession of Bob:

[0224] (0.29188884, 0.73412345).

[0225] Upon receiving the vector (z_1, z_2) from Bob, Alice calculates the vector (k'_1, k'_2) by the formula:

[0226] $(k'_1, k'_2)=(\{z_1 \cdot a_0 + z_2 \cdot a_1\}, \{- z_1 \cdot a_1 + z_2 \cdot a_0\})$

[0227] with the precision K + D = 10 decimal places after dot:

[0228] (k'_1, k'_2)=({0.35875809966422024 8·48176925 + 0.43055384716003046 7·18034725}, {-0.35875809966422024 8·18034725+ 0.43055384716003046 7·48176925})=

[0229] =({17283862.060665664071377 4+ 7764920.231223180463966575}, {-6470103.668966804512111 8 + 20742760.403090250806373975})=

[0230] =(0.2918888445, 0.7341234463)

[0231] Since this vector is (K, D)-consistent (i.e., its first coordinate has digits 4 and 5 at 9^{th} and 10^{th} places after dot, and its second coordinate has digits 6 and 3 at 9^{th} and 10^{th} places after the dot), the vector (k'_1, k'_2), being rounded to the first K = 8 digits of each coordinate, constitutes the geometric key in possession of Alice:

[0232] (0.29188884, 0.73412345).

[0233] Thus, the vector (0.29188884, 0.73412345) is the geometric key shared by Alice and Bob. This key can be used in any major symmetric cryptosystem.

[0234] The invention has been described with reference to a particular preferred embodiment, but variations within the

spirit and scope of the invention will occur to those skilled in the art. For example, it will be understood that the public information $g=(g_1, g_2)$, D, N, K of the system can be stored on any suitable media, for example a "smart card," which can be provided with a microprocessor capable of performing arithmetic operations so that the keys can be distributed to and/or from the smart card.